

EMPLOYEE NAME: _____

AGENCY/DIVISION: Human Services/Appeals and Regulations

CLASSIFICATION TITLE: State Program Administrator, Coordinator (unclassified)

WORKING TITLE: DHS Privacy Official

POSITION CONTROL NUMBER: _____

POSITION PURPOSE: To serve as the point person for DHS' compliance with the data privacy requirements imposed by the federal Health Insurance Portability and Accountability Act (HIPAA); to develop, coordinate, document and implement privacy policies and procedures that comply with HIPAA; to handle requests for health data and document disclosures; to provide extensive training for both DHS employees and business partners on compliance with HIPAA privacy standards; to develop contracts between DHS and business partners that establish the permitted and required uses and disclosures of individually-identifiable health data, in compliance with HIPAA standards; and to develop sanctions, investigate complaints about disclosures and apply sanctions if employees or business partners misuse individually-identifiable health information.

REPORTS TO: Administrative Law Manager
Appeals and Regulations Division

DIMENSIONS: As both a Medicaid agency and as a direct provider of health services, the Department is required to meet all of the technical standards of HIPAA within 26 months of publication of federal regulations. Publication of the regulations regarding privacy is anticipated before the end of calendar year 2000. To meet these standards will require coordinating efforts with other state and county agencies, private insurers, and medical providers. Failure to meet these requirements can lead to legal liabilities and possible federal sanctions.

CLIENTELE: DHS staff from all program divisions and state operated services; 87 county human service agencies; the Minnesota Department of Health; the Department of Children, Families and Learning; the Department of Administration; the Attorney General's Office; private insurers and medical providers; and legislators and legislative staff.

EMPLOYEE'S SIGNATURE _____ DATE _____

SUPERVISOR'S SIGNATURE _____ DATE _____

	<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
	A	30	A
I. PRINCIPAL RESPONSIBILITY			
Lead the department wide effort to develop and implement administrative, electronic and technical and physical safeguards to protect the privacy of health information, including a new electronic data system to track disclosures of individually identifiable information within the timeframe imposed by the HIPAA privacy regulations.			
TASKS			
1. Provide the Department with legal expertise on the data privacy requirements imposed by the federal Health Insurance Portability and Accountability Act (HIPAA)			
2. Develop, document and implement privacy policies and procedures that comply with HIPAA.			
3. Coordinate activities between the program professionals and information technology professionals (MMIS and MAXIS, PRISM and SSIS) in order to ensure that DHS meets HIPAA compliance requirements.			
4. Perform an inventory of current safeguards for health data and determine whether they are sufficient to meet HIPAA privacy standards.			
5. Develop procedures for verification of the identity and authority of persons requesting health information.			
6. Develop a notice to be provided to individuals, informing them of their rights regarding health data and how the Department intends to use or disclose their individually identifiable health data.			
7. Develop a process to be used by policy divisions within the Department to review the accuracy of data which is to be released.			
8. Coordinate all efforts and advice with data practices attorney, to ensure consistent applications of HIPPA and Minnesota Government Data Practices Act.			
9. Monitor developing state and federal case law as it pertains to HIPAA, and oversee implementation of required data collection, storage or dissemination changes.			

	<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
II. PRINCIPAL RESPONSIBILITY	A	20	A

To represent the Department on state and federal legislative issues related to compliance with HIPAA privacy standards.

TASKS

1. Provide technical assistance to Department staff from affected program divisions who are drafting legislation relating to compliance with HIPAA privacy standards.
2. Coordinate legislative activities regarding legislation related to compliance with HIPAA privacy standards, contact legislators and legislative staff and provide technical assistance as requested, and draft or provide testimony as requested.
3. Monitor all legislation relating to compliance with HIPAA privacy standards, prepare bill analysis as requested, attend committee hearings, and testify at committee hearings as necessary.
4. Report to federal government concerning DHS' compliance with HIPAA privacy standards.

<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
A	10	A

III, PRINCIPAL RESPONSIBILITY

Provide legal analysis of questions and issues relating to release of healthcare data under HIPPA standards. Handle requests for health data and document disclosures.

TASKS

1. Serve as the Department=s single point of entry contact person responsible for receiving requests for health data.

- A. Make determinations as to whether the request meets the Aneed to know@ or other minimum tests.
- B. Make determinations as to which policy area the data request fits into.
- C. Document the rationale for the request and determine if it is valid.
- D. Make determinations as to whether the requested data should be disclosed.
- E. Delegate the data requests to the appropriate division for completion.
- F. Document the disclosures of information at the individual level.

2. Provide individuals with an accounting of disclosures of their identifiable health information.

3. Serve as the contact person responsible for receiving complaints about disclosure of health data.

<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
A	15	A

IV, PRINCIPAL RESPONSIBILITY

Coordinate efforts between DHS and other state agencies to ensure that shared private healthcare data is being collected, stored and disseminated in accordance with HIPAA.

TASKS

1. Develop and/or participate in interagency committees to ensure that shared healthcare data is being collected and stored uniformly and consistent with HIPAA requirements.
2. Provide extensive training for both DHS employees and selected business partners on compliance with HIPAA privacy standards.
4. Provide initial training for all DHS staff on the general requirements for compliance with HIPAA privacy standards.
5. Provide new employees with information on the general requirements of HIPAA privacy standards.
6. Provide training, as requested, for program divisions on specific aspects of compliance with HIPAA privacy standards.
7. Develop electronic training modules on compliance with HIPAA privacy standards for use by DHS employees and selected business partners.
8. Monitor to assure that employees and business partners complete required training on compliance with HIPAA privacy standards, and sign a certification following completion of training.
9. Coordinate all training activities with Data Practices Attorney.

<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
A	15	A

V. PRINCIPAL RESPONSIBILITY

To develop contracts between DHS and business partners (private healthcare providers, contractors, and counties) that establish the permitted and required uses and disclosures of individually-identifiable health data, in compliance with HIPAA standards.

TASKS

1. Establish connections via meeting and committees with business partners to lay the ground work for effective contract negotiations.
2. Develop a model contract for DHS to enter into with all business partners that assures that the business partner:
 - A. Will not use or further disclose protected health data other than as permitted or required by the contract.
 - B. Will not use or further disclose protected health data that would violate the requirements of HIPAA if DHS were to disclose the data.
 - C. Will use appropriate safeguards to prevent use or disclosure of protected health data other than as provided by its contract.
 - D. Will report to DHS any use or disclosure of protected health data not provided or by its contract of which it becomes aware.
 - E. Will ensure that any subcontractors or agents to whom it provides protected health data received from DHS agrees to the same restrictions and conditions that apply to the business partner with respect to such data.
 - F. Will, upon termination of the contract, return or destroy all protected health information it receives from DHS and retain no copies of such information.
3. Negotiate HIPAA compliance contracts with business partners on behalf of DHS

<u>PRI.</u>	<u>%</u>	<u>DIS.</u>
A	10	A

VI. PRINCIPAL RESPONSIBILITY

To develop sanctions for misuse of individually-identifiable health information.

1. Develop procedure for informing the public of their rights under HIPPA.
2. Develop procedures for investigating complaints, including any necessary forms or notices.
3. Work in conjunction with human resources representatives to develop disciplinary sanctions for misuse of individually-identifiable health information by DHS employees.
4. Develop sanctions for business partners who misuse individually-identifiable health information.

NATURE AND SCOPE

Ultimately, this position will be responsible for ensuring that all of DHS is in compliance with the HIPAA privacy regulations. The position holder will interpret the HIPAA regulations and direct other DHS professional staff in their implementation of those regulations. This individual will coordinate activities between the program professionals and information technology professionals (MMIS and MAXIS, PRISM and SSIS) in order to ensure that DHS meets HIPAA compliance requirements. Additionally, s/he will develop and/or participate in interagency committees to coordinate efforts between DHS and other state agencies to ensure that shared private healthcare information is being stored and disseminated appropriately. Administrative duties will also include meetings with private contractors and health care providers, and business partners, coordinating with them to ensure that information sharing and dissemination is consistent and in conformity with regulations. The position holder will represent DHS before the state legislature, and respond to inquiries from the federal government concerning HIPAA compliance. This position will also be responsible for developing sanctions for violations of HIPAA, which will involve complex and delicate negotiations with those same public and private stakeholders, including advocacy groups and the general public.

This position reports to the Administrative Law Manager within the Appeals and Regulations Division. Oral and written communication is used to carry out responsibilities. Within the Department, communication and coordination is required with all staff, including the commissioner, deputy commissioner and assistant commissioners, chief executive officers of the state operated services, division directors, and other department staff. This position must establish and maintain working relationships with staff from the Minnesota Departments of Health, Administration, and Children, Families and Learning, as well as staff within the Attorney General's Office. This position must also establish and maintain working relationships with staff from county human service agencies, and with other public and private organizations and individuals within the health care industry.

KNOWLEDGE AND SKILLS

The classification requires knowledge of: law and administrative procedures sufficient to serve as a technical expert before departmental policy committees, governmental agencies and other public forums; public policy principles and administration; project planning and operations; negotiation tactics; DHS information technology and technology resources; and qualitative and legal analysis. Additionally, the position requires effective communications skills, sufficient to clearly communicate, develop, understand, persuade, motivate, and collaborate with and lead others.

The individual in this position must be licensed to practice law in the State of Minnesota. S/he must possess extensive knowledge of Administrative Law and Public Welfare Law, including knowledge of federal and state statutes, regulations and policies relating to health care and data practices. Knowledge of HIPAA (Health Insurance Portability Accountability Act) is essential.

The person holding this position must have an understanding of the department's business

environment, and possess skill in negotiating complex solutions to programmatic and technical problems. He/she must clearly communicate complex information to the highest levels of the department as well as collaborate with technical specialists working on Department computer systems.

The position must be able to identify statutes and rules that apply to individual situations, and advise members of the welfare system of the legal consequences for actions or failures to act in compliance with HIPAA. The position must also be able to determine the impact of proposed or adopted changes in state or federal law, rule or regulation that affects release of health data, and advise and inform legislators and departmental staff of the consequences of proposed or adopted changes.

Strong communication skills are essential for this position, as are human relations skills, as the position is required to relate to a diverse group of individuals with a wide range of knowledge and responsibility.

PROBLEM SOLVING

Problems of a complex nature will need to be resolved by the person in this position. The position holder must be able to analyze the nature and classification of the health data in question, and the status of the person or entity requesting the health data; determine which provision(s) in HIPAA apply to the data; determine if other laws, rules or regulations are in conflict with the applicable provision of HIPAA; determine if there are court decisions that address the issue; and recommend procedures or processes that reduce or eliminate the conflicts in law and assure compliance with applicable statutes and regulations.

FREEDOM TO ACT

The position functions with considerable independence, reporting activities to the director or manager on an exception only basis for most tasks. S/he must exercise independent judgement consistent with applicable law. The individual in this position consults with the DHS Data Practices Attorney and the Attorney General's Office regarding complex or unusual questions of law, or when related litigation is anticipated.